STATE OF MARYLAND

State of Maryland
Department of Budget and Management
Statewide Security Support
Standard Operation Procedures for Electronic Evidence Handling

November 13, 2002

Prepared By:
Tim Appleby, Senior Engineer/Analyst

Science Applications International Corporation
13921 Park Center Road, Suite 300
Herndon, VA 20171

SAIC-6099-2002-140

Prepared For:
Carmella Thompson, Assistant Director of Security
Department of Budget and Management, Office of Information Technology
45 Calvert Street
Annapolis, MD 21401

OFFICIAL USE ONLY

TABLE OF CONTENTS

INDRX OF FIGURES

INDEX OF TABLES

1. INTRODUCTION

In an effort to increase the overall statewide security capabilities, the State of Maryland is developing and implementing a comprehensive statewide security program. This effort consists of four primary tasks that include the development of a statewide incident response capability. An integral part of this capability is the proper handling of electronic evidence when investigating any incident.

1.1. Purpose of This Document

This document will act as a Standard Operating Procedure (SOP) for collecting, handling and maintaining various forms of electronic evidence when responding to an incident. This Standard Operating Procedure represents a subset of the overall Incident Response Methodology found in the document titled State of Maryland Security Incident Response Capability (IRC) Plan, Document Control Number: SAIC-6099-2002-088. This document was developed to ensure consistency in incident handling procedures throughout the state.

1.2. Policy/Authorization

The creation and operation of a State of Maryland Computer Incident Response Capability is authorized per the references below; the IRC is a key component of the State's IT security program, which is a component of the statewide IT standards, policies, and procedures.

The Maryland Code, Law Pertaining to Information Processing, State Finance and Procurement, Title 3, Subtitle 4, 3-401 to 3-413 authorizes this capability. Section 3-403 (a) charges the Secretary, DBM, with responsibility “for developing, maintaining, revising, and enforcing information technology policies and standards.” Section 3-410 authorizes the Chief of Information Technology (also known as the State CIO) to carry out certain duties for the Secretary, DBM. Section 3-410 (d) (1) charges the State CIO with the responsibility to the Secretary of DBM for carrying out the duty of “developing, maintaining, and enforcing statewide information technology standards, policies, and procedures.” The State CIO has created the Security and Architecture Division within the Office of Information Technology of the Department of Budget and Management to assist the State CIO. The Deputy Director for Security of the Security and Architecture Division has caused this capability to be implemented.

1.3. Intended Audience

This document is specifically intended for use by authorized State of Maryland Incident Response Personnel including tier one, tier two and tier three analysts. This document may also be used to support any State personnel authorized to perform electronic media incident handling activities in support of an investigation.

1.4. Document Organization

This document will provide background information regarding electronic evidence, examine the needs and requirements pertaining to proper handling during an investigation, and identify a procedure to be used whenever incident response activities require electronic evidence extraction.

2. BACKGROUND

In the course of any incident response activity, the collection of evidence to support an investigation is inevitable. The quantity and types of evidence required in any investigation may vary depending on the complexity, severity and sensitivity of the incident. Evidence gathering provides the cornerstone for any investigation and improper handling may provide adverse consequences. Proper handling becomes especially important if an incident resolution requires intervention by the courts. As mentioned above, this document will examine a process for identifying, collecting, transporting, storing and documenting electronic forms of evidence. These guidelines will provide a uniform procedure to be utilized during any investigation requiring evidence extraction.

2.1. Electronic Evidence

According to the Department of Justice, electronic evidence is any information and/or data that is stored on, or transmitted by an electronic device. As such, electronic evidence is considered latent evidence in the same sense that fingerprints are considered latent evidence. This means that in its natural state, the evidence that is contained within the physical object (for example, a hard drive) is not visible by the individual handling the evidence. For this reason, additional equipment or software may be required to make the actual evidence “visible”.

In the course of an investigation, appropriate care must be taken to preserve the integrity of the processes used to obtain and secure evidence as testimony may be required to explain the examination process and any process limitations. For this reason, each incident responder must understand the fragile nature of electronic evidence and the principles and procedures associated with its collection and preservation. The goal is to prevent actions that may alter, damage, or destroy original evidence as this may compromise its validity if scrutinized by the courts. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion. In those cases where the likelihood of court scrutiny is good, a professional computer forensics person should be brought in to handle the evidence.

2.2. Types of Electronic Evidence

Evidence relating to an incident may surface in many different forms. Evidence may be stored in documents, logs, images, media files or a multitude of other data elements stored on one of a myriad of electronic devices. A single device collected as evidence may house literally thousands of different forms of evidence and care must be taken to protect the integrity of that data. The following is a list of various types of electronic devices that may be included as part of an investigation relating to a network security incident.

2.2.1. Computer Systems

Computer systems represent the most common and expected form of electronic device through which electronic evidence will be collected. Care must be taken to ensure that the contents of the data residing on a computer system is not inadvertently altered or destroyed in the course of an investigation. When a computer system is designated as a piece of evidence, handling is determined by such factors as:

1. Type – The type of computer system relates to the make, model, brand and physical configuration.
2. Function – The function performed by a computer system being considered relates to whether it is a workstation used by an individual, or a server performing a process or function for others.
3. Current state – This refers to whether the system is on, off or in a state of hibernation. Additionally, this refers to whether the system is connected to a network or multiple networks.

Considerations:

The most common type of evidence collected in support of an incident will likely be media or log files on computer systems. The contents of these files must remain as pristine as possible to ensure that the information provides reliable insight into the events being investigated. For this reason, the following should be considered:

1. If a system is being considered for collection, the state of the system should be the first consideration. Even attempts to log into a system in standby mode will bring a system out of a state of hibernation, and may result in writing entries into the log files thus changing the contents of the drive (and evidence) significantly. Computer systems should be first photographed for documentation, and then turned off at a switch, plug or other power source to prevent unnecessary changes from occurring. If the system is connected to a network, care should be taken to ensure that it is not being used as a server or other processing resource.
2. Systems containing potential evidence should be identified and shut off prior to removing any peripherals plugged into the system. This will also ensure that entries are not written to the log pertaining to changes in hardware.
3. Any media should remain intact if the entire system can be removed as evidence. External media bays should be sealed with evidence handling tape, and documented with the collector's signature and the date and time of removal.
4. When removing any internal drives, all connections should be properly sealed and documented to prevent unauthorized tampering. Drive settings should remain unchanged including jumper settings and write protection.
5. Input devices should remain with computer systems to ensure compatibility when provided to the incident response team for analysis.

2.2.2. Access Control Devices

Access control devices provide authentication and access control to various electronic devices, computer systems, networks and applications. Access control devices typically contain digital credentials providing verification of a person's identity. These devices typically come in the following forms:

1. Smart Cards – Often used for financial transactions, smart cards store various identification data, digital certificates, keys and passwords on a small microchip.
2. Dongles – Similar to smart cards, dongles are small devices that plug into various external ports on computer systems to perform authentication and access control validation.
3. Key Fobs – Devices typically found attached to key chains or with employee identification badges, typically contain an LED display providing periodically updated random numbers. These random numbers are often used to authenticate remote users.
4. Biometric devices – A device connected to a computer system that performs authentication based on the physical characteristics of a user.

Considerations:

Access control devices, although not necessarily significant in and of themselves, may provide evidence of access (either authorized or unauthorized) to information relating to an investigation. The following should be considered when including access control devices as evidence:

1. Access control devices may or may not be stored with the systems or devices that they provide access to.
2. Batteries that have a finite life expectancy commonly power access control devices.
3. Typical access control devices interact with software residing on the system(s) being accessed.
4. There are three types of access control mechanisms based on security considerations. Single factor devices rely on one type of information for access control (something known such as passwords or pass codes), two factor authentication devices rely on two types of information to authenticate a user (something known and something possessed like smart cards), and three factor devices relate to three pieces of information for authentication (something known, something possessed, and something inherent to the user like biometrics).

2.2.3. Digital Cameras

Digital cameras are becoming more prevalent in the workplace with the growth in popularity of online collaboration and remote computing. These devices are typically capable of producing digital pictures and multimedia files that can easily be transferred from computer to computer for viewing or editing. Digital cameras may be dependant on the computer for storage and operation, or may in many cases provide internal storage on various forms of digital removable media.

Considerations:

Digital cameras may provide images pertaining to an investigation. When including a digital camera into evidence, the following should be considered:

1. Images produced by a digital camera are typically stored on compact volatile magnetic or optical media and stored either within the device, or separate from the device. Images produced with the camera may also be off-loaded to systems or media for back up or storage purposes because the compact media is limited in size.
2. Cameras depend on batteries and often have charging docks that provide recharging.
3. Cameras typically have various interfaces for connecting to various system ports, television and multimedia devices.
4. Additional media readers may be present on systems or printers for off-loading pictures for storage or output.
5. Some digital cameras, sometimes referred to as web cams, are mounted on the monitor or desktop and connected directly to a computer system providing a camera capability for Internet use. These web cams store information on the systems drives and should be considered a peripheral to the system.

2.2.4. Handheld Devices (Personal Digital Assistants)

Handheld personal devices, often called Personal Digital Assistants or PDA's for short have become extremely popular as a replacement to the daily organizer. These devices come in many styles, shapes, sizes and colors and are available from many manufacturers. Typically, these devices will allow a user to synchronize various content with computer systems through an interface cable or "cradle" that provides a freestanding pedestal for the device to plug into.

Considerations:

Handheld devices are available in many shapes and sizes, but typically fall into two general categories based on the operating system used. These are Palm OS and Non-Palm OS. When these types of devices are being collected as evidence, the following should be considered:

1. These devices typically synchronize with a host computer system, or multiple host systems. Content available on these devices may represent a subset, a replica, or a conglomeration of information from one or many other electronic sources.
2. Power for these devices is typically provided through batteries. Some use rechargeable cells, where others use disposable cells. It should never be assumed that the information would remain during long periods without battery operation.
3. Battery chargers, cradles and system interfaces are commonly found on systems used as hosts to these devices. All of these should be collected as evidence with the device.
4. Many handheld electronic PDAs have automatic power-up functionality when alarms are set. Care should be taken to ensure that the device is turned off, the infrared port (if available) is properly covered with opaque tape, and the cover is sealed to prevent contamination of data.

5. Many PDAs have wireless modems that allow access to Internet, email and other remote functions.
6. PDA’s storage or memory may be used to store files, documents, mail and other forms of digital media from the host system(s).

2.2.5. Electronic Organizers

Similar to Personal Digital Assistants, electronic organizers are devices used to maintain a small subset of the functionality found in most PDA’s. These devices are often used to store various names and addresses, calendar information, or phone directories.

Considerations:

Electronic organizers were commonly used as a predecessor to the PDA. These devices typically are stripped down handheld database files that are used to store specific personal information. When including a personal handheld organizer in an evidence collection, the following should be considered:

1. These devices usually operate on battery power. Information is typically volatile and should be considered at risk if battery power subsides.
2. These items may be found remote from any systems being collected and may not provide connectivity to host systems.
3. Organizers typically have non-removable internal storage with very limited capacity.
4. Organizers operating systems are typically proprietary and restrictive. Access to storage fields is likely limited to the fields designed for that particular device. Rarely are the drives on these devices used to store data from other hosts.

2.2.6. Hard Drives

Hard drives are magnetic storage mediums found in most computer systems. They come in a variety of storage sizes, but typically do not deviate significantly in physical dimensions. Desktop computer hard drives are larger than those found in laptops. Hard drives may be found internal to the computer or device, or external, depending on the circumstances.

Considerations:

Hard drives are typically collected as evidence if the system containing the drive cannot be removed. Considerations’ relating to drives being included for evidentiary collection may include:

1. Hard drives require a host system to function. The system provides power, software, and functionality through a specific type of interface.
2. Hard drives may be designed for IDE interfaces or SCSI interfaces.
3. Jumper settings should remain intact. These settings are designed to ensure that multiple drives can be used on one system (primary or slave) and their setting may represent evidence.

4. Drive dimensions for laptop drives tend to be smaller than desktop systems. The interface used to connect these drives also differs in size and configuration.
5. Hard drives are considered magnetic media and should remain away from any magnetic field that may cause destruction of data.
6. Ribbon cables should be removed from drive interfaces with care, as “pins” tend to be delicate.
7. Drive casings should never be removed as this may cause damage to the cylinders and tracks, and cause the drive to not function properly.

2.2.7. Memory Cards

Memory cards, for the most part are removable electronic storage devices that do not lose stored information when power is lost. Memory cards are typically used to store various forms of digital media such as digital images and music. They are used in a wide variety of devices including digital cameras, computers, PDAs and printers. They come in an assortment of storage capacities. Often, there will be a memory card reader in/or around the computer that allows direct access from the computer.

Considerations:

Memory cards are commonly found in multimedia devices such as music players, cameras, PDAs and electronic games. When included as evidence, the following considerations should be addressed:

1. Memory cards typically come in compact cards or “sticks” depending on the manufacturer.
2. Memory cards typically come in sizes ranging from 4, 8 16,32,64 or 128 MB.
3. Newer memory cards look like key chains and store information similar to a hard drive. These devices come apart and plug into the USB interface on a computer system.
4. Memory cards are considered “removable media” and require other electronic devices for power and to function.
5. Memory cards may be used to store any information found on a computer system including music, video, images, documents, or data.

2.2.8. Modems

Modems are devices that allow for communication between electronic devices through telephone lines, wireless interfaces, or other communication mediums. They may be internal or external to an electronic device.

Considerations:

Modems are common on mobile devices such as portable computers and handheld devices. The following considerations apply when including these devices as evidence:

1. Modems may be internal or external to the electronic device.

2. Modems may connect to telephone lines, cable lines, or wireless antennas to allow electronic devices to communicate.
3. External modems typically require an external power source and operate as a peripheral to a computer system using a variety of interfaces.
4. Modems operate at varying speeds.
5. Inclusion of a telephone modem in a corporate setting may indicate that an analog line exists, as modems require analog lines to communicate. This should be included as evidence if found present.

2.2.9. Network Components

Network components represent the various electronic devices that allow computers to interact over a network. Included devices are Network Interface Cards (NICs), hubs, routers, switches, firewalls, and cables connecting them to the network.

Considerations:

Network components mat come in a wide variety of forms. These may be cards used within electronic devices, stand alone systems connected directly to computer systems, or devices on a network maintained at a separate location from the evidentiary collection site. The following should be considered when dealing with network components:

1. A network component may be servicing multiple electronic devices. Care should be taken to understand what devices are connected to the network component to ensure that users external to an investigation are unaffected.
2. Many times a network device will not be movable due to operational considerations. In this case, the relevant evidence must be extracted from the device using a sound forensic methodology (which is beyond the scope of this document).
3. Many network devices are wireless and may appear disconnected.
4. Network devices should not be disconnected until the main power to the host device is off. This will ensure that evidence on the host device is preserved.
5. Some computer systems and electronic devices have infrared ports that allow networking to other systems or devices. These ports should be considered network components and secured with opaque tape to ensure evidentiary integrity of the host system.

2.2.10. Pagers

Pagers are small handheld devices that are used to alert a user when someone requests contact. Typical pagers allow for only numeric communications, but newer versions have alpha/numeric capabilities and may even facilitate two-way communication and email. Cell phones and PDAs can also be used as pagers. These devices all contain volatile information that may provide such as phone numbers, call logs, addresses, and personal data.

Considerations:

1. Most pagers operate on disposable or rechargeable batteries. Since batteries have a limited life, data could be lost if they fail. Therefore, a device powered by batteries is in need of immediate attention.
2. Information identified on the screen of a pager should be photographed, as it may not be stored when the device is turned off.
3. The pager may provide numeric or alphanumeric information and may provide either one-way or two-way communications.
4. Pagers often have identification information (i.e. Pin Number) on the outside case. This should be examined and photographed if possible.

2.2.11. .Printers

Printers rarely provide a relevant source for evidence collection unless the fact that one was available comes into question. In some investigations, it may be necessary to prove that a document was printed from a particular device or that access to that device was authorized. Printers typically do not provide any storage capability for historical, access control or operational logs. This type of information is typically handled on a print server (See Computer Systems). Some printers contain memory that may contain the last document(s) printed depending on the amount of memory available. Disconnecting the power will in most cases erase this memory.

Considerations:

If the printer is required for evidentiary inclusion, the following should be considered:

1. Printers may be connected locally or through a network or wireless type connection.
2. If a local connection exists, the printer may be connected to the host system through either a parallel cable or a USB cable.
3. If the printer is networked, it provides services for multiple clients and removal may disrupt service to other users.
4. Networked printers will either be connected to a print server or a network-printing device such as Hewlett Packard’s Jet Direct Card. These devices should be considered for inclusion as evidence if present.
5. Some devices contain infrared ports allowing printing to occur without a cabled connection to the printer. Care should be taken to ensure that the infrared port is adequately covered with opaque tape to prevent unintentional access or contamination of evidence.
6. Examine the printer to see if the last document(s) that it printed, can be printed again.

2.2.12. Removable Storage Devices and Media

Removable storage devices are storage devices that allow access to various forms of portable storage optical or magnetic media. Typically, they connect externally to a computer system through a cable interface, or are internal to the computer accessible from the case. Storage mediums and capacities vary and may be separate from the computer system. Some removable media is volatile, while others provide permanent data storage. These devices may or may not be connected to the computer system at the time of collection.

Considerations:

Removable storage devices provide portable storage to mobile workers. These devices come in many shapes, sizes and types. Devices and media are separate items that may be collected to provide evidence in an incident. These devices are typically used to store backups of system or operational data, multimedia files, images or other data needed in multiple locations.

As removable media depends on the appropriate storage device for operation, it is important to include these devices in an evidentiary collection to ensure proper access.

1. Some optical media such as CDRs written with Roxio’s Direct CD are written for use only with the specific device used to create the CD.
2. Some types of removable media are magnetic and may be destroyed if contact with other magnetic fields is made. Care should be taken to keep all electronic media away from speakers, magnets and electric motors.
3. Many forms of removable media have write protection mechanisms on the surface to protect accidental erasure or overwrite. The status of these mechanisms should be documented and remain unaltered for analysis.
4. Most removable media has protective cases and labels that may prove useful in an investigation. These may or may not contain the media and should not be overlooked.
5. Removable media stored in a system being collected as evidence should remain in the unit and sealed with evidence tape.

2.2.13. Scanners

Scanners are devices that allow printed materials to be copied in a digital format for use on computers. Scanners are external to the computer system and connected through a cable interface. Some scanners are included within printers and may not be immediately recognized as such. Additionally, many scanners provide the ability to use the computer to fax paper-based documents to remote fax machines or computer systems.

Considerations:

Scanners may provide evidence regarding information found on a system or device. Scanners may be used to digitize information when system based access or storage is necessary. The following should be considered when dealing with scanners as evidence:

1. Scanners may be found as flatbed, path-through, or handheld variants.
2. Scanners are often found in all-in-one office appliances providing printing, copying and fax capabilities.
3. Scanners typically attach to a local port on a computer system through a cable. Types and lengths of cable may vary based on location and type of scanner.
4. Many scanners utilize Optical Character Recognition (OCR) software allowing editing of physical documents with word processors.
5. Many scanners have built in memory that may hold an image of the last thing scanned. This image will be lost if power is removed from the scanner.

2.2.14. Fax Machines

Fax machines are devices that allow printed materials to be copied in a digital format for transmission to a computer or another fax machine. Fax machines can be either internal or external to a computer system and connected through a cable interface. Some fax machines are included within printers or as part of a computer modem and may not be immediately recognized as such.

Considerations:

Fax machines may provide evidence regarding information found on a system or device. Fax machines may be used to digitize information when system based access or storage is necessary. The following should be considered when dealing with fax machines as evidence:

1. Fax machines may be found as flatbed, path-through, or internal fax-modems.
2. Fax machines are often found in all-in-one office appliances providing printing, copying and fax capabilities.
3. Fax machines typically attach to a local port on a computer system through a cable. Types and lengths of cable may vary based on location and type of scanner.
4. Many fax machines have built in memory that may hold an image of the last thing faxed. This image will be lost if power is removed from the device.

2.2.15. Telephones

Many analog, digital and cellular telephones now have the capability to store information in memory. Stored information may include a name and address book, frequently called numbers, a history log, periodic reminders, and other personal information that may be valuable for an investigation.

Considerations:

Most workers utilize analog, digital or cellular phones for business or personal reasons. Information stored on these devices may provide information relating to an investigation. The following should be considered:

1. Most business facilities offer phone services to employees through a centrally controlled switch. Phones tend to be digital and all logs, records and configuration files are stored on the switch.
2. Cellular users may store information locally. Cellular phones operate on battery power and may or may not retain information once the battery wears out.
3. Cellular phones come in two varieties; IS41 that contain all user al information within the physical handset, and GSM which store all user operational information in a smart card or chip. US phones are typically IS41, but frequent travelers may have GSM or hybrid variants.
4. Some phones provide advance functionality through wireless Internet access. Additional services may include web surfing, email, web calendaring and Internet contact lists.
5. Some cellular phones have infrared ports to synchronize with various electronic devices including PDAs, computer systems, and handheld organizers.
6. Phones that are not part of a centrally located switch are typically analog and may have additional input interfaces for data. These types of phones typically store personal information in a small internal storage capacity.
7. Additional devices used for performing identification of incoming calls (CallerID) may also be available to provide historical records of incoming phone activity.
8. Most newer cell phones maintain a record of the most recent calls dialed, missed and received. Cell phone statements can also be used to identify calls made and received.
9. Office phone switches may also contain a call log of calls made, and received.

2.2.16. Miscellaneous Electronic Items

Any other forms of electronic devices that may contribute answers in an investigation should be considered for inclusion. Items of interest may include various forms of input devices used to communicate directly with an electronic device, interface cards used to attach electronic devices together, communication devices providing connectivity between electronic devices, and storage mediums not covered above used to store relevant files. Electronic devices such as music jukeboxes are being manufactured to interact directly with computers and provide huge storage capacity. These devices may contain any type and kind of electronic information that may be relevant to an investigation.

Considerations:

This is a catch-all others category that is used to accommodate anything not covered in one of the categories above. For this reason, the most important consideration here is what additional items to include as evidence.

1. As a rule of thumb, any electronic device, item that supports an electronic device, or item created using an electronic device may fall under this category.
2. After collecting all of the relevant devices available, it is important to ensure that any supporting items are also included to ensure that the data can actually be retrieved for analysis. Items such as power supplies, PCMCIA cards and dongles, interface cables, input devices, docking stations and port replicators should be included with the supported devices.
3. Paper output should be collected if produced on printers, fax machines or adding tapes previously collected as evidence.
4. Other electronic devices such as micro recorders, calculators and dictation devices may also add information relevant to an investigation.

3. PROCESSES

As mentioned above, an effective incident response capability relies heavily on proper incident handling procedures to ensure that the findings are unbiased and that they represent a true and accurate picture. For this reason, evidentiary handling requires various equipment and supplies to ensure proper chain of custody, storage and transport. Depending on the specifics of the incident, the types of evidence being gathered, and the logistics of the selected devices, evidence handlers may require any of the following:

Heavy-duty sealing tape to be used for securing cartons, envelops, or various other forms of containers. Many products of this type are designed specifically for evidentiary gathering and may provide a writable surface to provide a signature and other documentation. NOTE: If plain sealing tape is used, care should be taken to ensure that the surface is marked for tamper reduction. The surface should be labeled with some form of permanent ink with the signature and date. The tape should be placed so that the item cannot be tampered with without it being very evident that the tape was disturbed. It does no good to just tape the drive bay door, if the entire case could be opened and the drive accessed in that manner.

1. Adhesive tagging labels designed to maintain documentation in support of chains of custody. These labels are available in many shapes and sizes depending on the evidence being collected.
2. Various corrugated and plastic containers to transport and store evidence during collection. Items may include media pouches, boxes, folders, envelopes and pouches. These should all be easily sealable, free from visible damage, and provide quick and definitive evidence that the item being sealed has been tampered with.
3. A digital camera and new memory card should accompany the collector to preserve the state of equipment prior, during and after collection occurs. Procedural disputes may require proof of proper handling if the results of an investigation are questioned. There is no substitute to a picture in support of proper documentation.
4. A standard electronic tool kit containing various non-magnetized tools for removal of screws or other connectors should be available. When removing various electronic devices, the use of various tools may be required for removing screws, plugs and cable ties. These tools should include small and large Phillips and straight head screwdrivers, various sized hex tools, tweezers, scissors, and a surgical style knife.

The various processes that make up the incident handling response are discussed below.

3.1. Evidence Collection

When responding to incidents, proper evidence collection may be paramount to the success or failure of obtaining inconclusive proof of wrongdoing, indications of probable cause, or indications of activity relating to an incident. Depending on the specifics relating to an incident, evidence collection may be handled in many different ways and require the collection of numerous types of electronic devices, files and systems. Specifics of an investigation and the nature of the evidence being gathered may require differing forms of collection. One incident may require the collection of logs, rules and back-up data pertaining to a production server, whereas another may require a gathering of electronic equipment in an employee's office. Regardless of the scope of the evidence collection, the following should always be followed to ensure that the information's integrity remains intact:

1. The site where any evidence is being obtained should be secured from unauthorized access as soon as possible to ensure that the contents remain unchanged.
2. An attempt should be made to retain evidence in a form which closely resembles it's original. When possible, original evidence should be collected for purposes of an investigation.
3. Evidence should always be secured, sealed and tagged using procedures described below.
4. Analysis should never be conducted during the collection stage of an incident. This may significantly alter the evidence rendering it ineffective. Analysis should always occur on duplicates of the original evidence collected.
5. Only authorized individuals should be allowed access to evidence. Chain of custody documentation should be performed during any change-of-hands pertaining to the original evidence.
6. Evidence should always be secured as soon as possible in a medium that protects its contents from unauthorized access, corruption or destruction of the data, or accidental omission from an investigation.

3.2. Evidentiary Integrity Assurance

Above all, the most important goal in proper evidence handling involves the overall integrity of the devices and information collected. Integrity includes not only the physical well-being of the devices, but the operational integrity of the stored data and the methodological integrity of the chain of custody and documented processes used to conduct the investigation. In order to insure that the evidence offers the best possible information to incident handlers, the following guidelines should be followed at a minimum to protect the integrity of the investigation:

1. The site of the evidence collection should be secured from unauthorized access before and during the collection.
2. When applicable, digital pictures should be taken providing details relating to the evidence being gathered prior to collection.
3. Selection of all appropriate evidence should be conducted prior to any actual collection. This should include a detailed inventory of devices being considered.

4. Devices should be removed from the site according to the considerations outlined above. Care should be taken when deciding whether to unplug a device from either power or network access.
5. Devices being collected should be secured for transport using security tape, evidence bags and boxes.
6. Security tape should be properly labeled according to the documentation requirements listed below.
7. Site should be reexamined for any portable or mobile media that may be stored separate from devices. These include compact discs, floppies, tapes, optical discs, portable players, zip and jaz drives, access cards or other items that may contribute to an investigation of a security incident.
8. If actual devices cannot be removed, pictures of the device should be taken to show system status at time of collection.
9. If storage devices are required to be removed, proper forensic methodologies should be utilized. The scopes of these methods are outside of the scope of this document.
10. If at any point, evidence is not retained within your immediate possession, it is important to ensure that it is stored in a secure area that is inaccessible from unauthorized access, that this precaution is well documented, and that some form of validation exists to ensure that the location is secure. This may be a log from an access device, a camera, or a trusted authorized individual standing watch over the location.

3.3. Documentation Requirements

Proper evidence collection requires vigilance related to thorough documentation. Documentation of items, processes and activity related to evidence collection initiatives are necessary to ensure proper chain of custody, evidence of procedural integrity, and historical accounts for future requirements. Documentation typically begins the moment that it is decided that evidence handling is required in an investigation. Typical data required during the collection process includes:

1. The name, title and location for the evidence collector.
2. The date and the location the evidence is being collected from.
3. A complete description of each item to be included into evidence including make, model, serial number, capacity (if known), quantity, and descriptions of any visual details that are noticed.
4. Pictures of all items are recommended to ensure consistence before and after collection. These pictures may include various angles, screen shots and general site shots for documentation.
5. A description of the process used to disengage, disassemble and package any electronic evidence providing a time based account of any activity pertaining to the collection. This should include timestamps when each action was taken.

All documentation should be considered as evidence and handled in the same manner as the evidence collected. It should be stored with the evidence and protected from modification using similar tactics as those described above. Documentation should be consistent among investigations and should follow an authorized format. An example Inventory form is included in Appendix A as well as an internal inventory form in Appendix B.

3.4. Storage and Transport Requirements

To ensure the safety and integrity of evidence collected in support of an investigation, it is important to apply caution when packaging, transporting and storing various forms of electronic equipment. As indicated earlier, electronic evidence tends to be rather fragile and requires a significant amount of care to protect its integrity and ensure proper preservation. Evidentiary storage requires vigilance not only at the time of collection, but throughout the investigative process. For this reason, the following guidelines should be supported depending on the particulars of the investigation.

1. When evidence is collected, various photographs are important not only to document a before and after state, but also to ensure proper setup for examination and assessment. Cable placement is one example of information that may be used to re-assemble digital equipment at a lab or state facility. In order to ensure investigative integrity, proper (same as original) cable placement is imperative. Additional steps to ensure proper evidence handling are colored stickers matching cables to interfaces, various sized plastic bags to hold smaller media, and adhesive tabs for identifying any observable damage or anomalies.

2. All digital evidence should be sealed in a proper sized carton, bag or envelope and packed tightly with foam, paper or other forms of non- abrasive packaging materials to ensure damage free transport.

3. Either a safe transport media device should occupy any open storage bays, or blank media designed for the particular drive should be placed in the open bays. This will ensure that the heads of the drive are parked during transport to avoid damage.

4. A detailed inventory worksheet (Appendix B and C) should accompany any evidence stored in a single carton, bag or envelope. This inventory should be signed by the collector, and verified once opened by an authorized responder.

5. All cartons, bags and envelopes should be sealed with heavy-duty reinforced packaging tape and signed and dated using a permanent marker. Forensic evidence tape can be purchased for this requirement.

6. Each carton, bag or envelope should be labeled with the words “FRAGILE” and “HANDLE WITH CARE”. This will hopefully prevent damage if the items are being shipped, or are handled by others. Any deviations in handling should be fully documented for chain of custody.

7. Items being transported by collector should remain in his/her possession at all times. If third party shipping methods are used, the cartons should be properly labeled and numbered. If third party shipping is being used (not recommended if

avoidable), collectors should remain in possession of packages until physically received by shipping authority. If possible, a signature of possession should be obtained from shipping authority.

8. Once delivered to site of destination, cartons should always be properly examined for damage, evidence of tampering, or other anomalies not present at the site of origin. Observations should be recorded. If possible, pictures of boxes should be taken showing integrity of carton and seal.
9. When opening carton, bag or envelope, care should be taken if using sharp instruments. Sealing tape should remain on package to preserve evidence of process. Never remove sealing tape from package.
10. Items contained in packages should be verified against the accompanying inventory listing. Care should be taken to ensure that all information matches package contents (i.e. Serial Number, Make Model…) Inventory list should be updated to include confirmation of contents or variations observed. Receiving person(s) should sign and date inventory worksheet to preserve chain of custody.

3.5. Evidentiary Retention

Once the evidence is delivered to the destination site, proper safeguards must be taken to ensure proper preservation of evidence. Physical, virtual and procedural safeguards are needed to ensure that original evidence is protected from contamination. In order to ensure these requirements, the following safeguards should be in place:

1. All original evidence should be recorded, examined for damage or observed anomalies, and stored in a protective safe. This safe should only be accessible by authorized incident responders and provide compartmentalized storage to accommodate multiple investigations.
2. All original documentation relating to a particular investigation should be stored in the safe with its corresponding evidence. Original evidence and documentation should never be modified once stored in this manner.
3. A log should be maintained to ensure chain of custody is maintained during and after an investigation. This log should include verification of removal, access, and submissions to the safe.
4. The safe should be located in a protected area with acceptable means for authentication and access control. A record of access should be maintained and preserved indefinitely.
5. This room should provide reasonable protection from various forms of damage such as fire, water, heat, cold or humidity.
6. The safe should be secured to either the floor or wall if it can be removed from the premises by reasonable means.
7. All investigative and analytical work should be performed on forensically obtained copies of original evidence, which should be appropriately labeled as such and stored along with its original counterpart when not being used.

8. Evidence should always be removed from workspaces when not in use, even when working in a secured setting. This may prevent unauthorized persons from accidentally coming in contact with evidence.

9. Electronic evidence should never come in contact with magnetic devices or fields. Care should be taken to ensure that tools and other items used to access these devices are intended for electronic use, as many possess magnetic properties.

10. All electronic copies may be stored to various forms of optical or magnetic mediums for backup and archival purposes once an investigation ends.

11. Archival and backup evidence may be stored at secured and authorized facilities after an investigation ends. This will ensure available space for future incidents, and allow for long-term retention if further analysis is required. Proper record retention requirements should be determined but is specifically outside of the scope of this document.

APPENDIX A: EVIDENCE INVENTORY WORKSHEET

Evidence Inventory Worksheet	
Date:	Investigation Name and Number:
Start Time: End Time:	Address of Evidence Collection:
Collection Agent and Phone Number:	City and State:
	Internal Site Location:
□ Computer running at the time of entry?	
□ Computer connected to network? Network connection disconnected?	
□ Phone line connected to computer? Modem disconnected?	
□ Screen of the computer photographed or content noted (comments below)?	
□ Computer location and connections photographed and/or labeled?	
□ Safepark or blank diskettes placed in all unoccupied drives? Optional: If Safepark – powered on to park the hard drive?	
□ Machine booted or examined – See forensics handling guideline (Incident Response Specialist)	
□ Computer case opened? (Use internal parts worksheet) (Incident Response Specialist)	
Room # Where Collected:	Description of where found in room:

Evidence Tag No.:	Description:	Markings on Front:	Manufacturer:	Serial No.:	Model No.:
	COMPUTER Visible Drives • 3.5 Drive • 5.25Drive • CD ROM • TAPE • Other				
	Monitor				
	Keyboard				
	Mouse				
	Modem				
	Printer				

Additional Comments:

APPENDIX B: INTERNAL PARTS INVENTORY WORKSHEET

Internal Parts Inventory Sheet							
Investigation No.:				Date:			Initials:
				Computer ID:			
Evidence Tag No.:	Qty:	Computer:	MB:		Manufacturer:	Model No.:	Serial No.:
		Fixed Drive					
		Fixed Drive					
		Fixed Drive					
			Occupied				
			Yes	No			
		Slot 1					
		Slot 2					
		Slot 3					
		Slot 4					
		Slot 5					
		Slot 6					
		Slot 7					
		Slot 8					

Additional Comments: (Switch settings, markings, listing of bad tracks, monitor switches, etc.)